DoH and DoT Server Discovery

& Deployment Considerations for Home and Mobile Networks

https://tools.ietf.org/html/draft-btw-add-home

March 2020

M. Boucadair (Orange)
T. Reddy (McAfee)
D. Wing (Citrix)
N. Cook (Open-Xchange)

Agenda

- Scope & Objectives
- Target DoT/DoH deployments
- Which discovery information?
- The discovery procedure
- Rogue servers
- DoH-specific: one pending issue
- Next steps

Scope

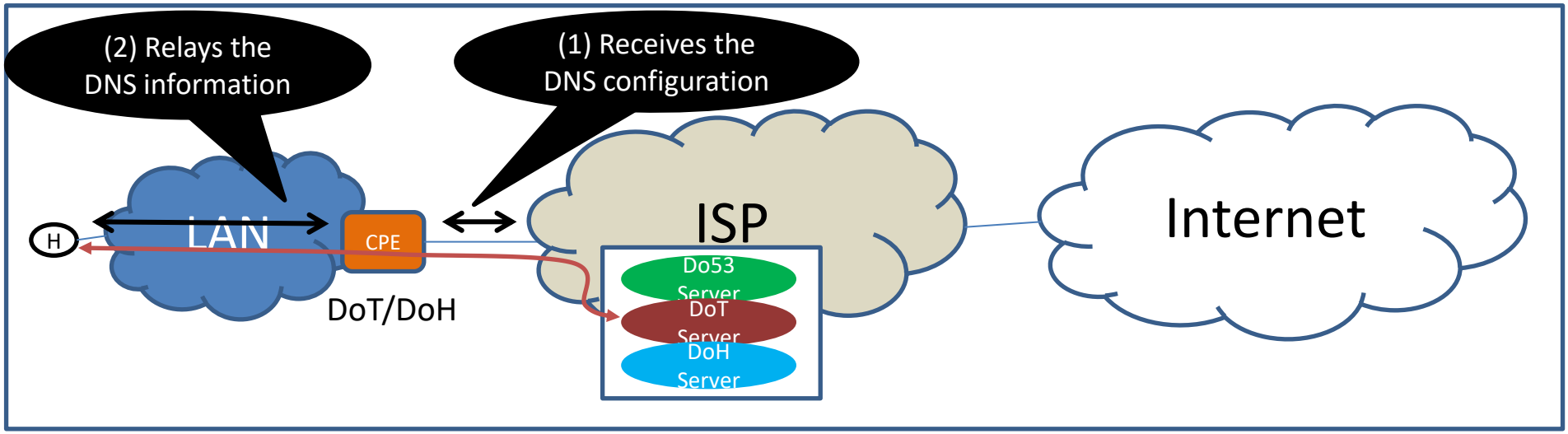
Excerpt from the ADD WG Charter:

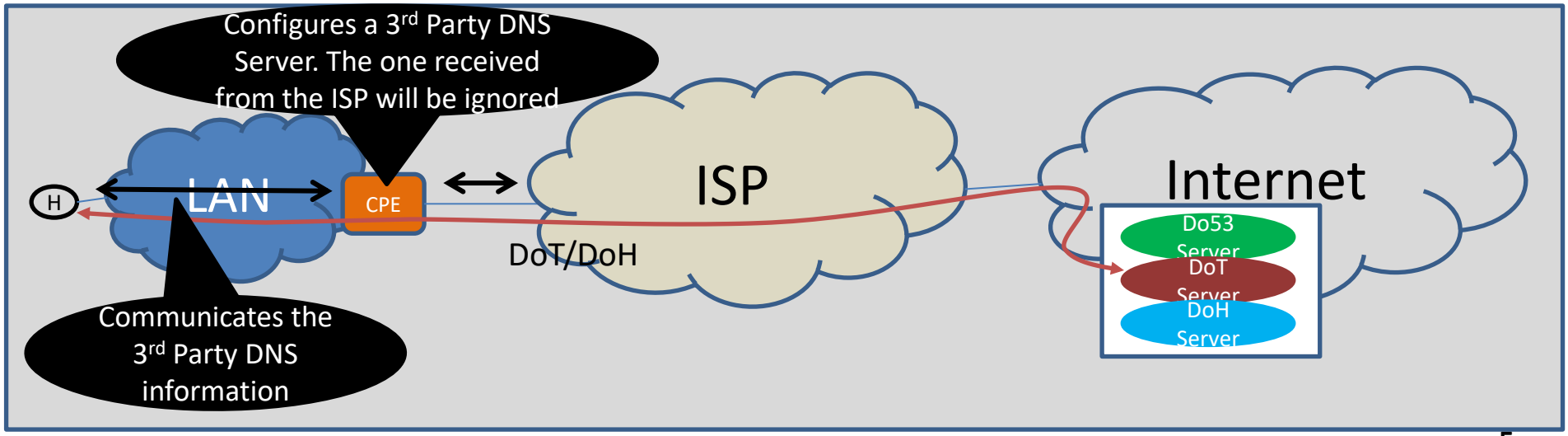
"Define a mechanism that allows clients to discover DNS resolvers that support encryption and that are available to the client either on the public Internet or on private or local networks."

Objectives

- Discuss DoT/DoH deployment considerations for **home networks**
  - Both Home and Mobile networks
  - ISP, public, and private resolvers
  - Enterprise networks are out of scope
- Specify the required **server discovery mechanism(s)**
- Sketch the **required steps** to use DoT/DoH capabilities provided by local networks

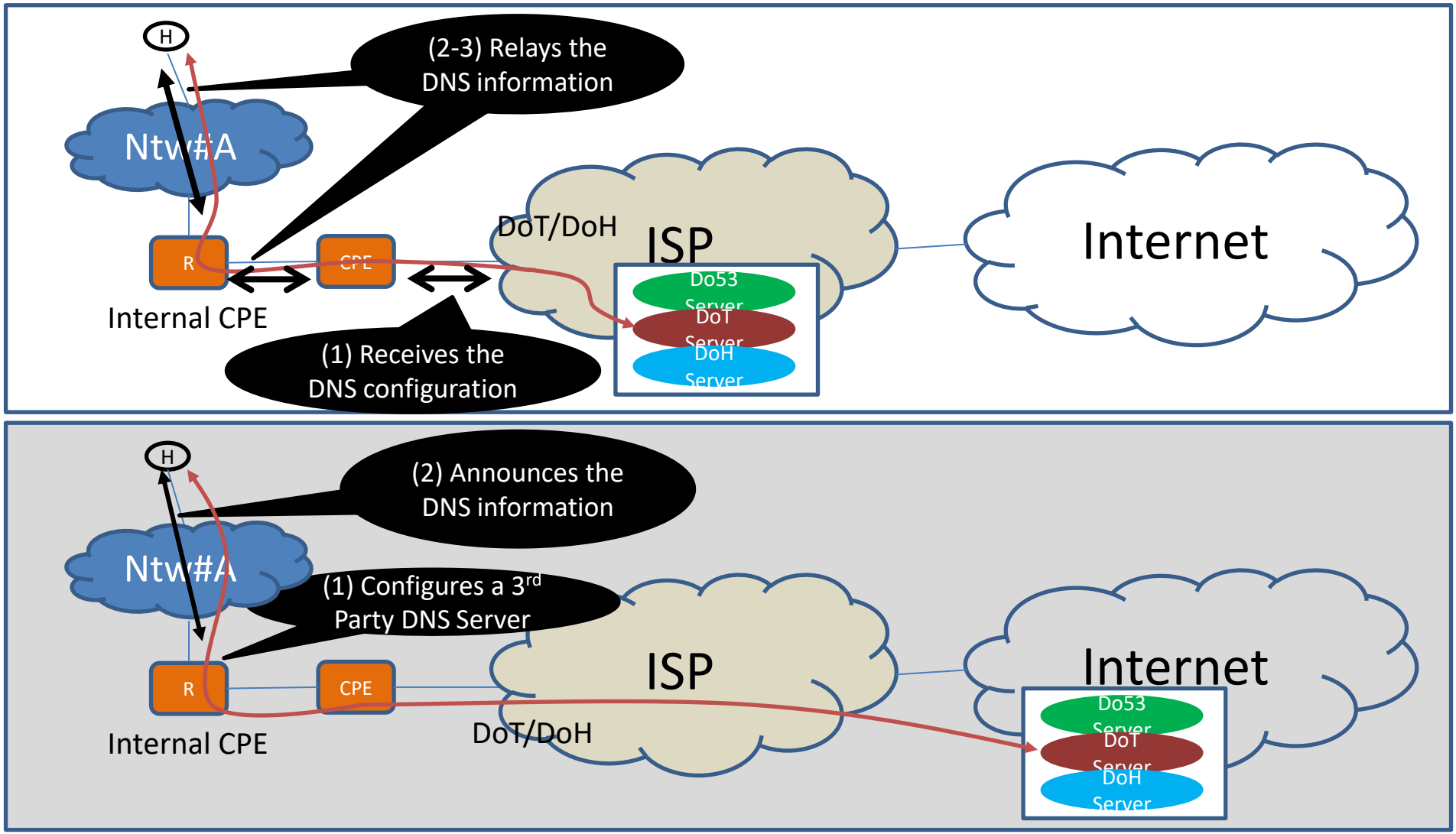
Sample Encrypted DNS Deployments: Managed CPEs



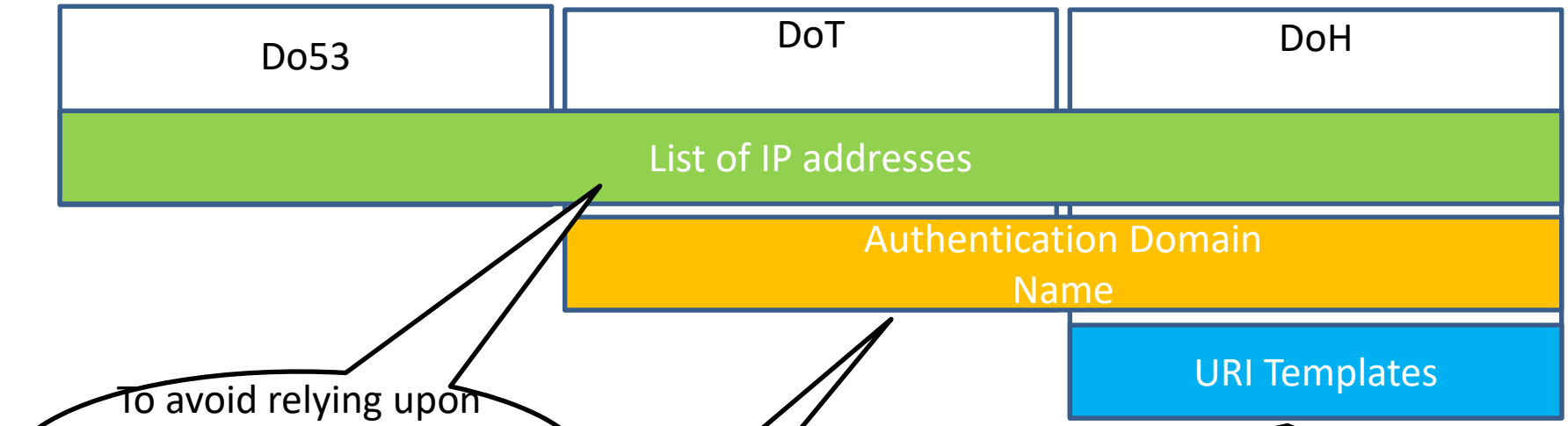


DoT/DoH: Means DoT and/or DoH

Sample Encrypted DNS Deployments: Unmanaged CPEs



Which Discovery Information is Needed?

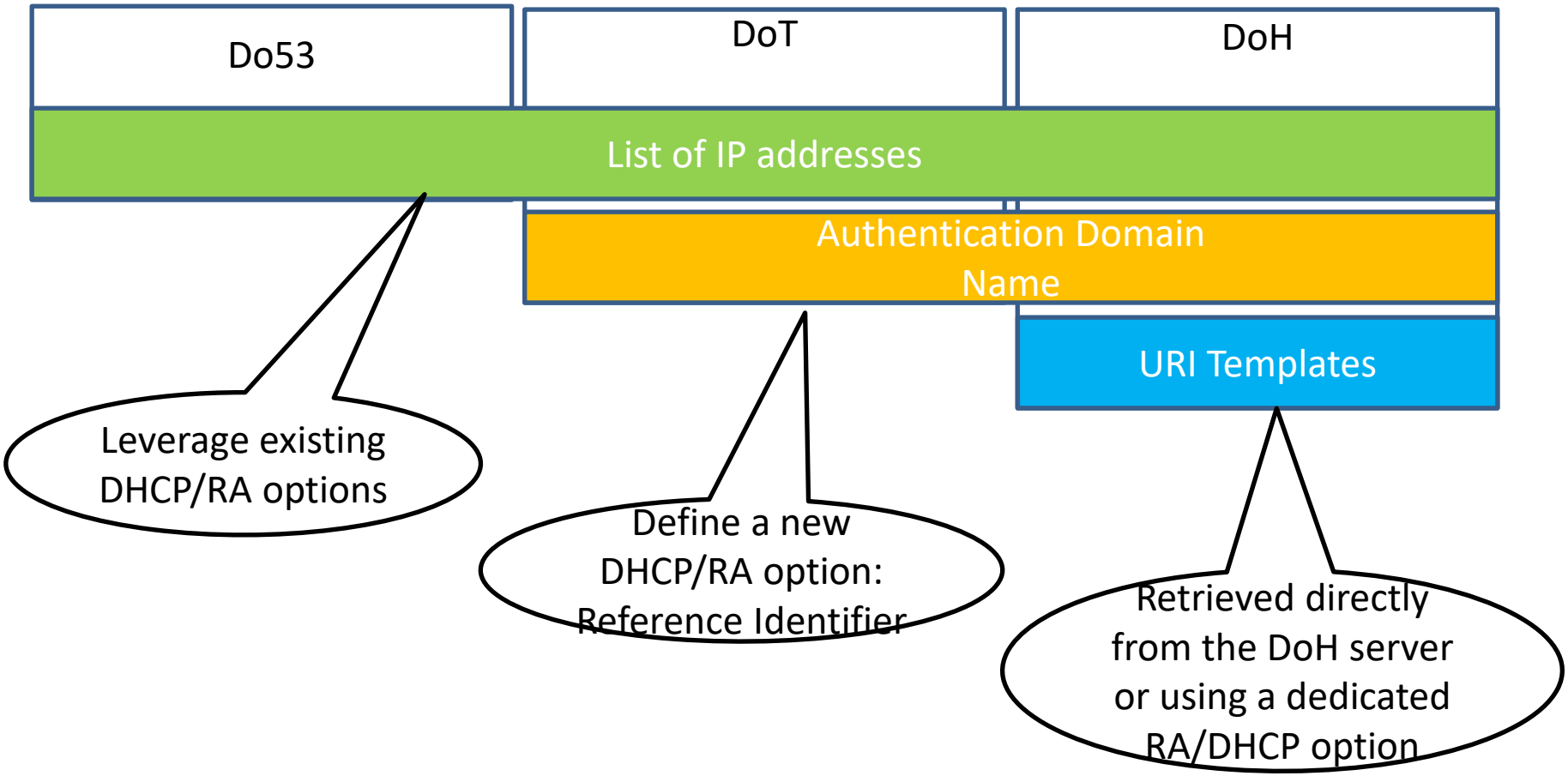


To avoid relying upon Do53 or opportunistic profile to resolve the resolver's name

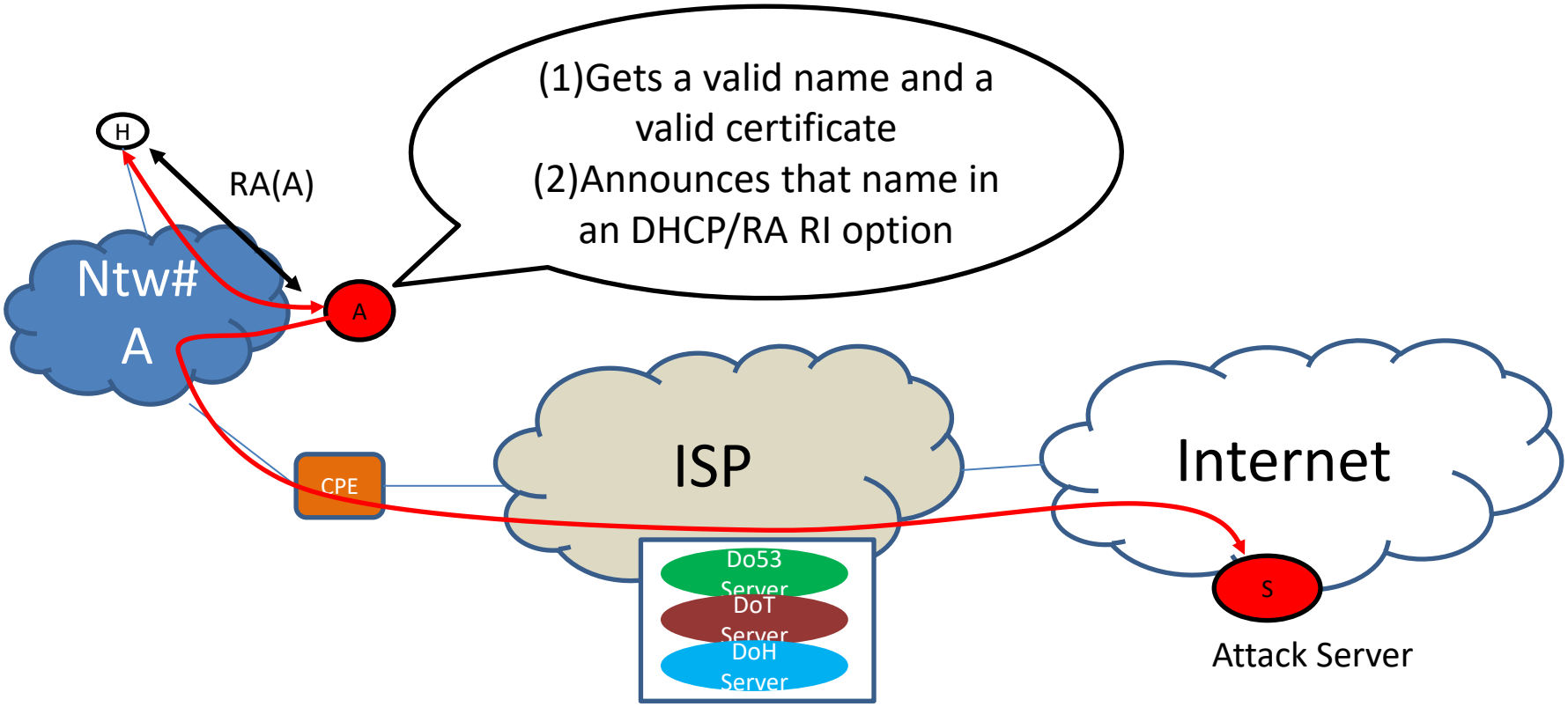
For PKIX authentication

1. How to construct the URL to use for resolution
2. Other URI variables may be supported in the future
3. DoH resolvers may expose customized services: no-filtering, filtering+malware detect, filtering+adult block, …

Which Channel for Discovery?

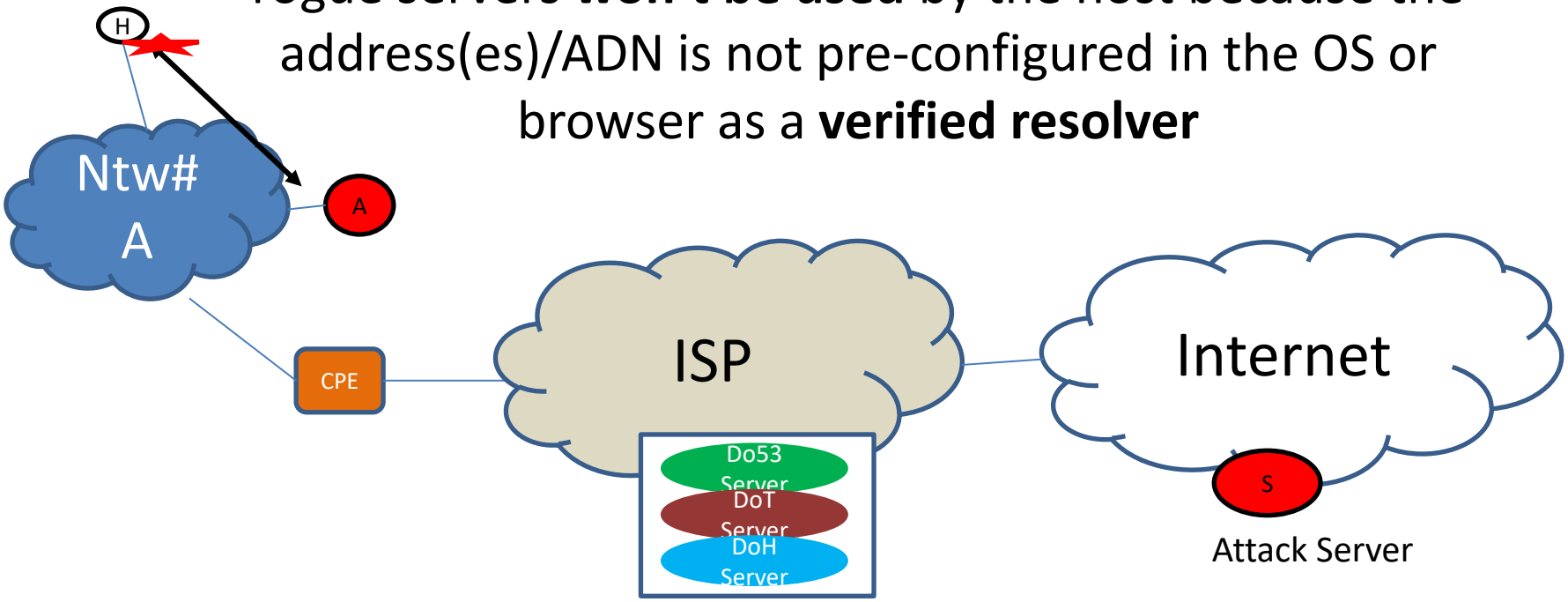


What about Rogue Servers?



Rogue Servers Will be detected

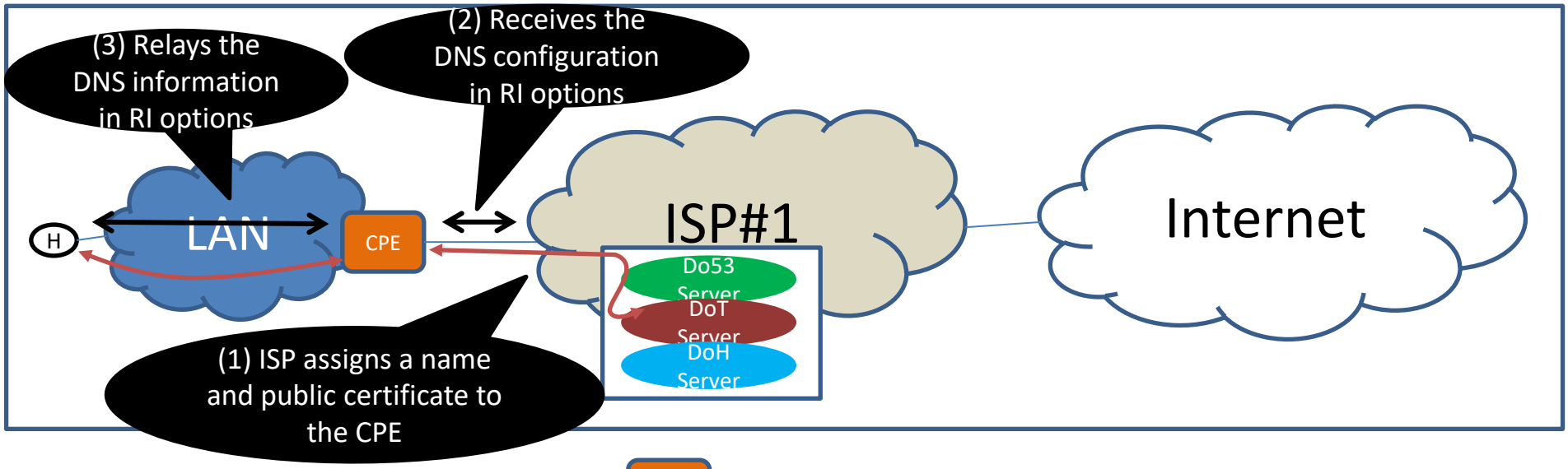
DNS servers conveyed in RA/DHCP messages from rogue servers **won't be used** by the host because the address(es)/ADN is not pre-configured in the OS or browser as a **verified resolver**

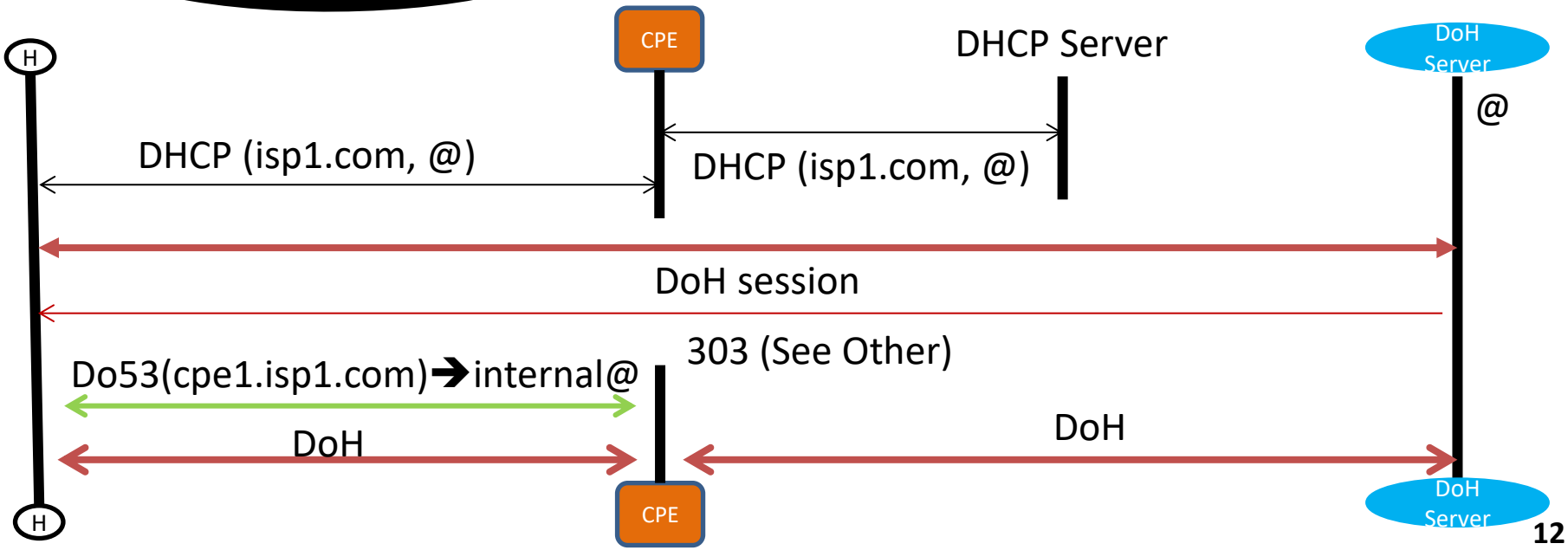


Verified Resolvers

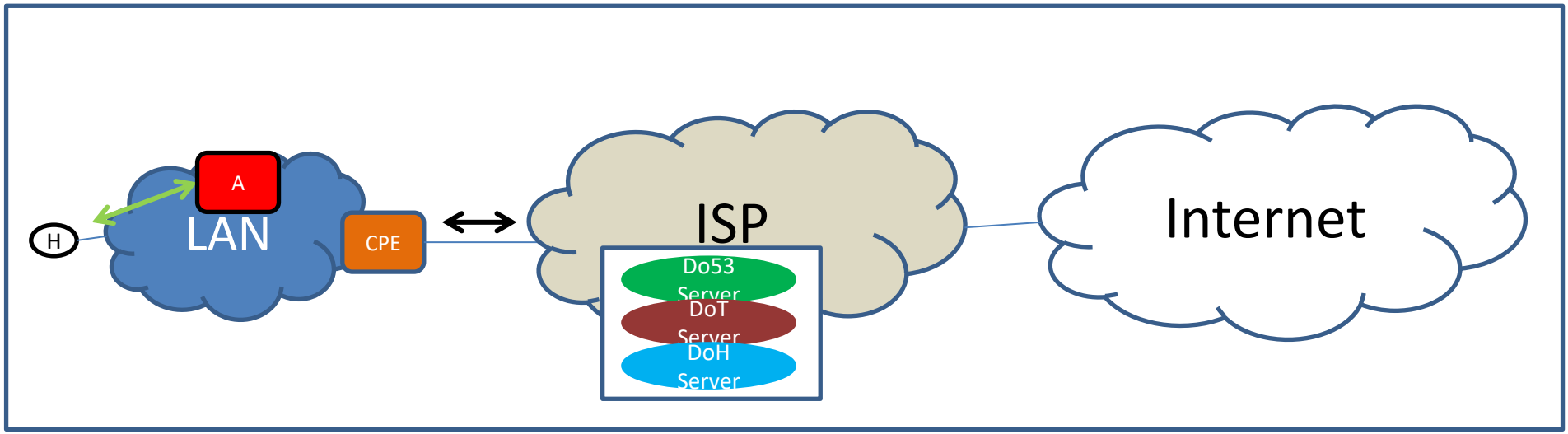
- Auto-upgrade
  - If the **DNS server's IP address** discovered using DHCP/RA is pre-configured in the OS or Browser as a verified resolver, the DNS client auto-upgrades to use the pre-configured DoH/DoT server tied to the discovered DNS server IP address
  - If the **ADN** conveyed in DHCP/RA is pre-configured in the OS or browser as a verified resolver, the DNS client auto-upgrades to establish a DoH/DoT session with the ADN
- Other approaches are discussed in the draft, e.g.,
  - If the discovered DoH/DoT server is not pre-configured in the OS or browser, the client may validate the signatory (e.g., cryptographically attested by the ISP)

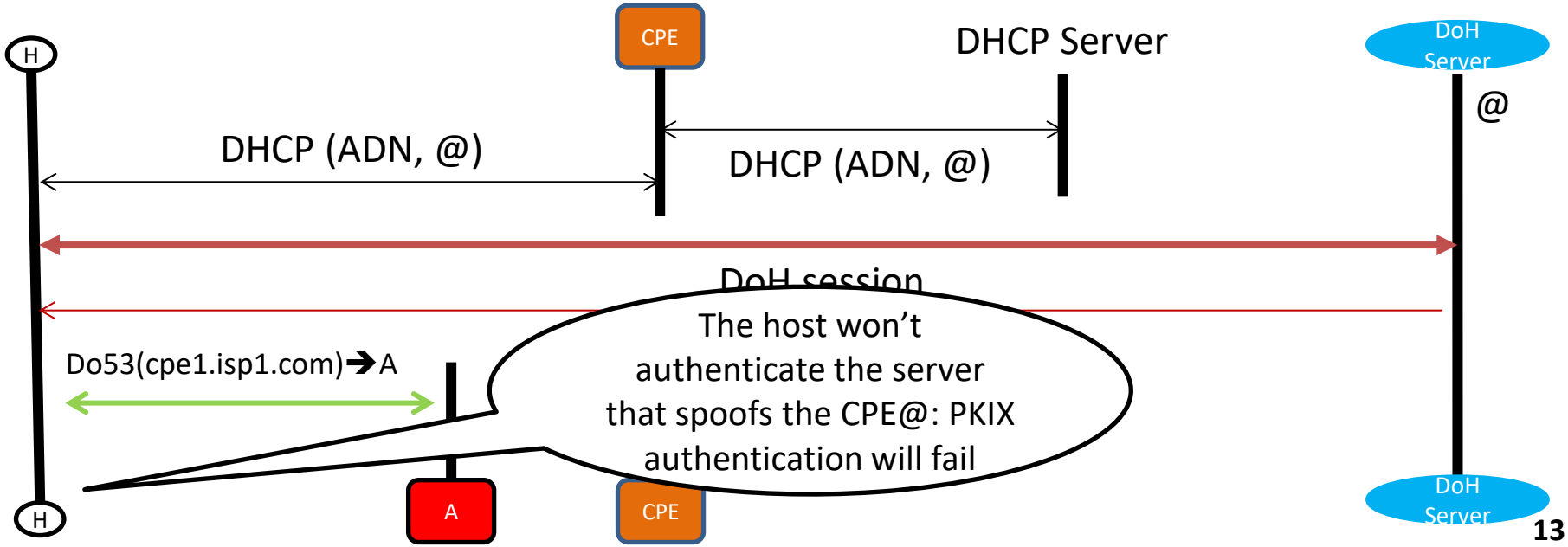
Host a Forwarder in a Managed CPE





Do53 for Redirect: **Not a** Threat





DoH Services & URI Templates

- Why?
  - RFC8484 supports URI templates with “dns” as the only variable, but future extensions may allow for queries with **other variables**
  - DoH resolvers may host **many services**; each identified by a URI scheme
  - DoH clients have to be instructed about **valid URI templates** to use
- How?
  - retrieved by querying a discovered DoH resolver
  - enclosed in a dedicated RA/DHCP option
- How the client uses these services is out of scope

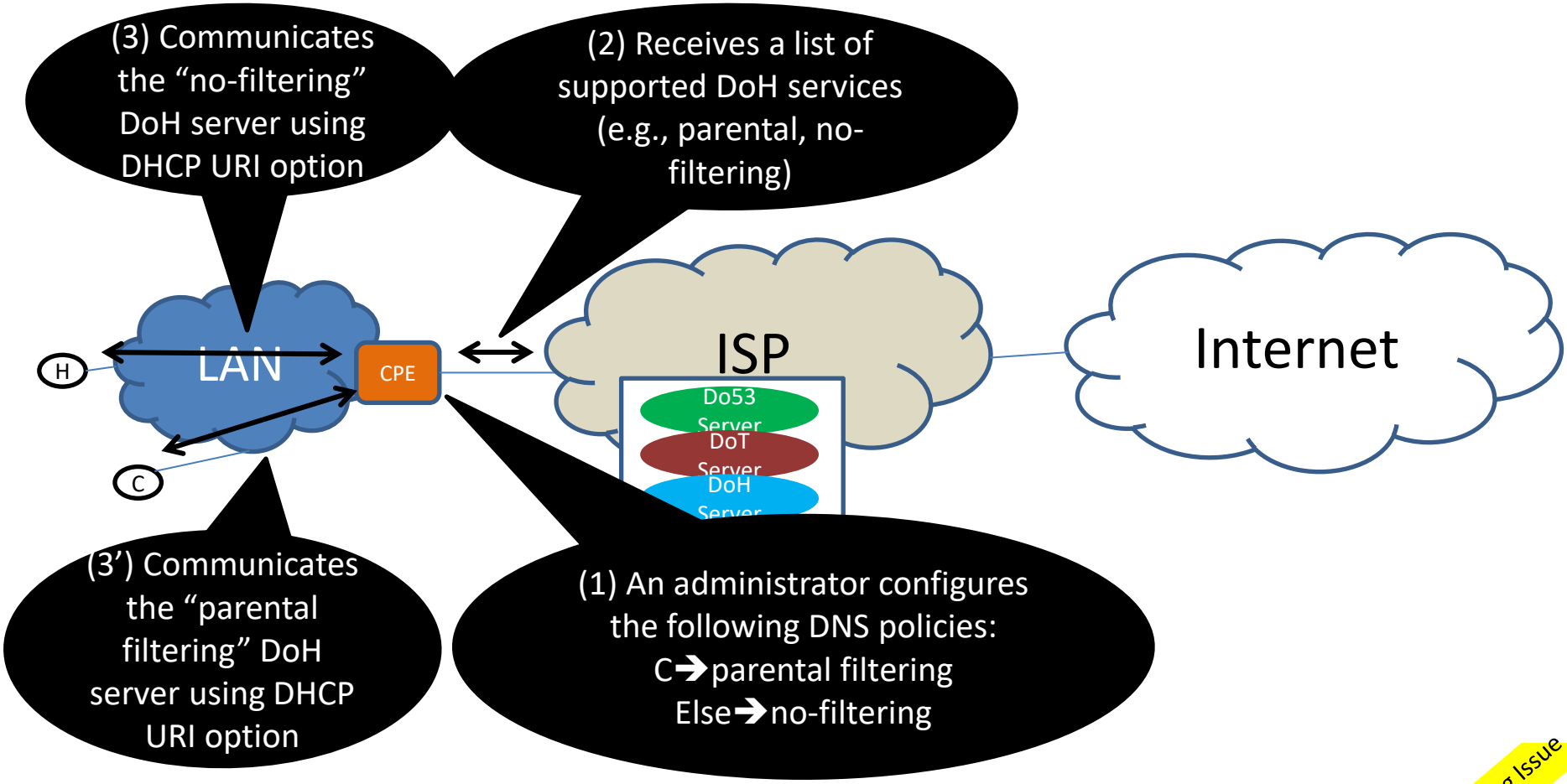
Pending Issue

URI Templates in RA/DHCP?

- Trade-offs are discussed in the document
  - Some Issues
    - Risk of stale information
    - Create a dependency between DHCP servers (access routers) and DoH resolvers
    - Need for an out of band mechanism if the DoH resolver is not managed by the ISP
    - May increase the size of RA/DHCP messages
  - Some advantages
    - Clients can immediately use the service(s)
    - Convenient if very few (stable) URIs are in use
    - Customized (local) configuration (See next slide)
- Do we need to pick one?
  - If yes, which one?

Pending Issue

Customized DHCP Configuration: An Example



Pending Issue

Implementation

- Ported DNSDist v1.4.0 with DoT/DoH support to OpenWRT-19.07

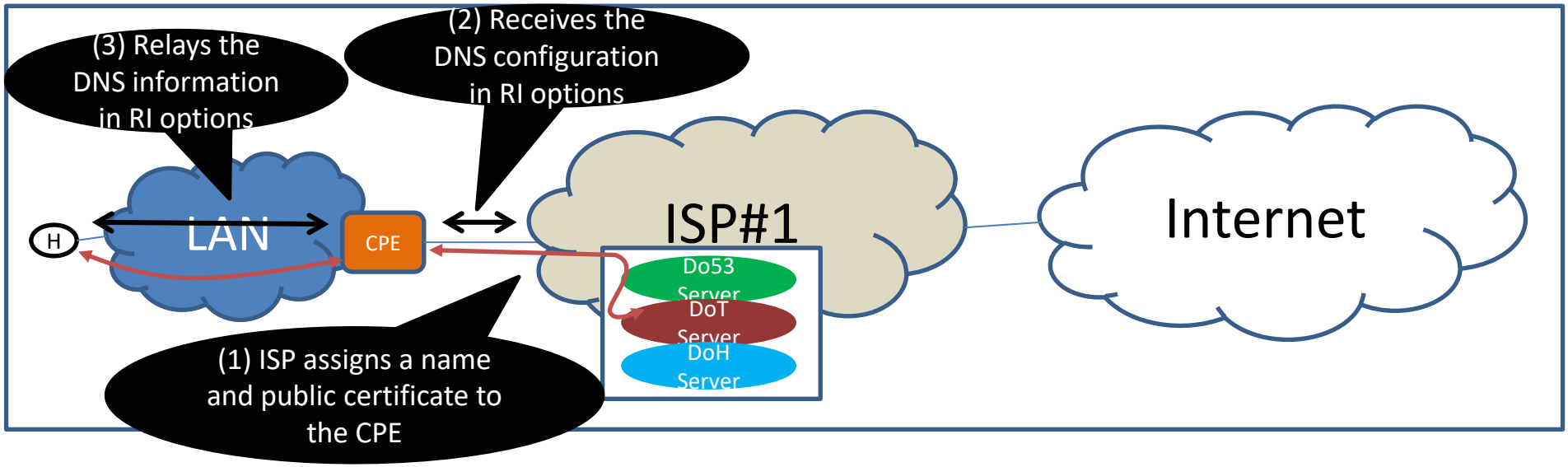
- Extended DNSDist to do DoT/DoH in the upstream (CPE to resolver)

Next Steps

- Need more feedback on the URI Templates discovery issue
- Consider adopting this document as a WG item
- Questions?

Appendix

Host a Forwarder in a Managed CPE



- Certificates are managed by the **ISP**
- ACME fully automates certificate management (e.g., certificate issuance, expiry etc.) and **no human intervention is required**
- ACME and https://letsencrypt.org/ (to generate certificates for millions of home routers) are already in place by some security vendors. No roadblocks is reported so far
- Certificates are pushed by ISPs to the CPEs

Multi-Interface Devices: Out of Scope